*1

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−25568

⑤1Int.Cl.⁵	識別記号	庁内整理番号
G 06 F 15/30	330	6798−5B
G 06 K 17/00	S	6711−5B
G 07 D 9/00	461 Z	7347−3E
G 07 F 7/12		8208−3E

⑬公開　平成3年(1991)2月4日

G 07 F 7/08　C

審査請求　未請求　請求項の数 1　(全4頁)

⑤4発明の名称　カード正当性確認方法

⑳特　願　平1−158420

㉒出　願　平1(1989)6月22日

⑦2発明者　古橋　寛仁　東京都港区虎ノ門1丁目7番12号　沖電気工業株式会社内

⑦1出願人　沖電気工業株式会社　東京都港区虎ノ門1丁目7番12号

⑦4代理人　弁理士　金倉　喬二

明　細　書

1. 発明の名称

カード正当性確認方法

2. 特許請求の範囲

1. オンラインシステムによってカードを利用して取引を行うに際し、そのカードの正当性を確認する方法において、

毎回の取引データによる処理終了毎に毎回異なるデータをカードとセンターファイルの両方に登録し、

毎回の取引開始時に両者のデータを比較照合することを特徴とするカード正当性確認方法。

3. 発明の詳細な説明

〔産業上の利用分野〕

本発明は、銀行等の金融機関やクレジットによるカードを利用するオンラインシステムにおいて、カードの正当性を確認する方法に係るもので、特に複製された偽造カードや同一内容のカードが2枚作成されて誤発行されたカードの早期発見を行うことができるカード正当性確認方法に関する。

〔従来の技術〕

従来、オンラインシステムにおけるカードの正当性の確認は、磁気ストライプやICによる内部の銀行コードや支店コード等の固定データやロジック(ICカードの場合)と個人データを組み合わせて作成した個有データを回線を利用して上位システムに送り、上位システム内部で上記の固定データや可変データを比較して等しいときにのみ正当なカードと認めていた。

〔発明が解決しようとする課題〕

しかし、上記のような従来技術によると、正当なカードの内容を複製された偽造カードがあることを発見する場合は、正当なカードの利用者が金融機関のカードにおいては残高の異常な不足、クレジットカードにおいては使用した金額と請求額との違い等によって判明するまで判らないものであった。

〔課題を解決する為の手段〕

本発明は、オンラインシステムによってカードを利用して取引を行うに際し、そのカードの正当

性を確認する方法において、毎回の取引データによる処理終了毎に毎回異なるデータをカードとセンターファイルの両方に登録することを特徴とする。

〔作　用〕

以上の構成によると、毎回の取引開始時に両者のデータを比較照合し、偽造されたカードが使用されても最後の取引処理に利用されたデータが合致しなければ取引が行われないことになり偽造カードの発見ができることになる。

〔実　施　例〕

以下に本発明の一実施例を図面を用いて説明する。

なお、以下の説明は銀行等の金融機関に置ける場合であり、また、カードはＩＣ内蔵のカードを用いた場合で説明する。

第１図は処理工程を示すフローチャート、第２図は取引処理装置のブロック図、第３図は上位システムの直前認証蓄積ファイル例の説明図、第４図はカード内メモリの構成図である。

第２図において１は取引処理装置、２はキーボード、３はＣＲＴ、４はプリンタ、５はハードディスク、６はＩＣ内蔵のカードとの通信制御装置である。

７は上位システムであるＣＰＵ，８はこのＣＰＵ７と上記取引処理装置１を結ぶ通信制御装置である。

ＩＣ内蔵のカード９は例えば第４図に示すようなメモリを有し、ＩＣ制御部、E^2ＰＲＯＭ、ＲＡＭ、ＲＯＭ等から成り、上記通信制御装置６を介して通信を行う。

以上の構成による本実施例の取引工程を以下に説明する。

Ｓ１　カードの取引処理装置１内への挿入による取引開始。

Ｓ２　取引処理装置１のキーボード２とＣＲＴ３によって取引の選択等の通常の初期処理を行う。

Ｓ３　カードの銀行コード、支店コード等を上位システムのセンターファイルに登録のものと比較して通常行われているカードの正当性の確認を行う。

Ｓ４　直前認証Ｄの送信要求をＩＣ内蔵のカードに送信し、ＩＣ内蔵のカードは第４図に示すような直前認証ＤをE^2ＰＲＯＭから読み取って上位システムに送信する。

ここで、直前認証Ｄとは本発明の要旨であり、例えば乱数等を利用し、カードを利用するたび（初期発行も含む。）に取引に関係しない文字等の記号により作成したカード利用毎に異なるデータであり、カードおよび上位システムのセンターファイルに登録したものである。なお、この直前認証Ｄの登録はカード処理のタイミング信号を利用して行うことで可能であるが、この方法に限るものではない。

Ｓ５　上位システムがカードからの直前認証Ｄを受ける。

Ｓ６　当該カードの前回利用時に与えた直前認証Ｄとセンターファイルに登録した直前認証Ｄとを比較する。

Ｓ７　その両者が等しくないときには当該カードは不正当なカードとして取引不成立となる。

Ｓ８　その両者が等しいときには上記Ｓ２で選択した取引処理を行う。

Ｓ９　乱数等から作成した新しい直前認証Ｄを上位システムのセンターファイルに登録する。

Ｓ１０　上記の新しい直前認証Ｄをカードに送信して登録して取引は終了する。

なお、上記実施例はＩＣ内蔵のカードの場合で説明したが、磁気カードでも同様であり、その場合には取引処理装置１に磁気ストライプのリード／ライト部が設けてあり、磁気情報によって上記直前認証の読み取り、書き込みが行われる。

以上説明した取引処理において、さらに直前認証一致後に暗証番号等で本人確認をするとカード利用の安全性は一層高まることになる。

なお、銀行コード等の通常行われているコードの正当性確認、直前認証確認および暗証番号等の本人確認はどれを先に行ってもさしつかえはない。

さらに上記実施例は、クレジットの取引においてもまったく同様に行われるものである。

〔発明の効果〕

以上詳細に説明した本発明によると、毎回の取引データによる処理終了毎に毎回異なるデータをカードとセンターファイルの両方に登録し、毎回の取引開始時に両者のデータを比較照合することにより、偽造されたカードが使用されても最後に利用されたデータが合致しなければ取引が行われないことになり偽造カードの早期発見が行われ、ひいては偽造の防止になる効果を有する。

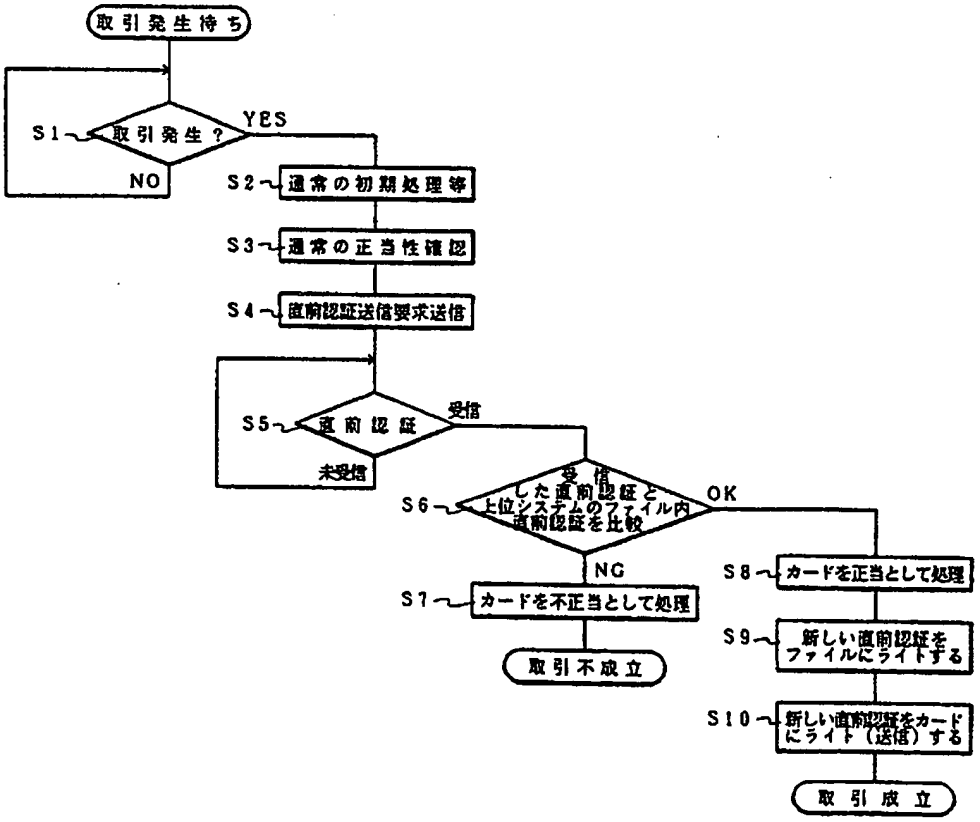
また、偽造カードが不正使用された場合、つぎに本物のカードを使用すると不正当なカードとなるなるために偽造カードが使用されたことがわかり、従来のように本来の使用者が気付くまで2枚のカードが生き続けるようなことがなくなり、これによっても偽造カードの早期発見が行われることになる。

4. 図面の簡単な説明

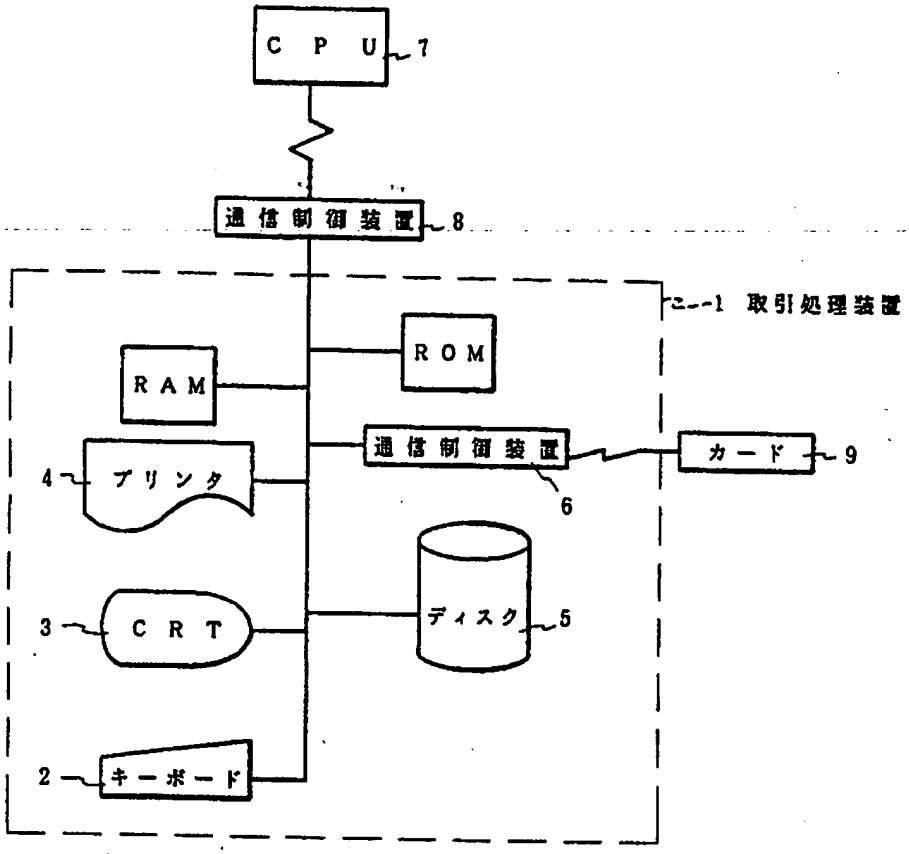
第1図は本発明の実施例を示す処理工程のフローチャート、第2図は取引処理装置のブロック図、第3図は上位システムの直前認証蓄積ファイル例の説明図、第4図はカード内メモリの構成図である。

1・・・取引処理装置
2・・・キーボード
3・・・CRT
6・・・通信制御装置
7・・・CPU
8・・・通信制御装置

特許出願人　　沖電気工業株式会社
代理人　　弁理士　金倉喬二

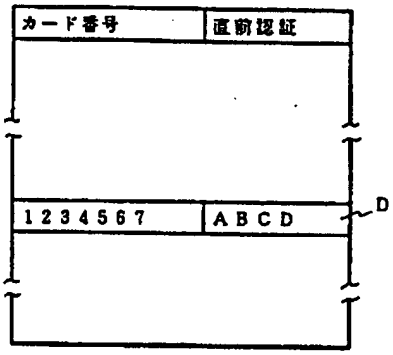


処理工程を示すフローチャート
第1図



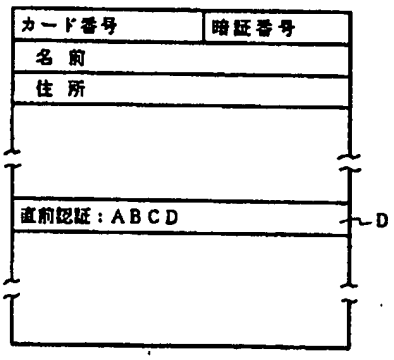
取引装置のブロック図

第 2 図



上位システムの直前認証蓄積ファイル

第 3 図



カード内メモリの構成図

第 4 図